Webinar Gratuito
OWASP WebScarab

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 30 de Enero del 2014

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
-  @Alonso_ReYDeS
-  pe.linkedin.com/in/alonsocaballeroquezada/

¿Qué es OWASP WebScarab?

WebScarab es un framework para analizar aplicaciones que se comunican utilizado los protocolos HTTP y HTTPS.

Fue escrito en Java y es portátil a varias plataformas. WebScarab tiene varios modos de operación, implementados por plugins.

En su forma de uso más común opera como un proxy de interceptación, lo cual permite modificar y revisar las solicitudes creadas por el navegador antes de ser enviadas al servidor, además de permitir modificar y revisar las respuesta devueltas desde el servidor antes de ser recibidas por el navegador.

WebScarab es capaz de interceptar una comunicación HTTP y HTTPS. Pudiendo revisar las conversaciones (solicitudes y respuestas) que han pasado a través de WebScarab

* https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

Características

Los plugins incluidos en WebScarab son los siguientes:

- **Fragmentos:** Extrae Scripts y Comentarios HTML desde páginas HTML cuando son vistos mediante el proxy, u otros plugins.
- **Proxy:** Observa el tráfico entre el navegador y el servidor web. Es capaz de observar tráfico HTTP y tráfico cifrado HTTP, negociando una conexión SSL entre WebScarab y el navegador y permite que pase a través de este un flujo cifrado.
- **Interceptación Manual:** Permite al usuario modificar solicitudes y respuestas HTTP y HTTPS al vuelo, antes de llegar al servidor o navegador.
- **Beanshell:** Permite la ejecución de operaciones arbitrariamente complejas sobre solicitudes y respuestas. Todo lo que pueda ser expresado en Java puede ser ejecutado.

Características (Cont.)

- **Revelar campos ocultos:** Algunas veces es más fácil modificar un campo oculto en una página por si misma, que interceptar la solicitud después de que ha sido enviadas. Este plugin simplemente cambia todos los campos ocultos encontrados en páginas HTML a campos de texto, haciéndolos visibles y editables.

- **Simulador de Ancho de Banda:** Permite al usuario emular una red lenta, para poder observar como el sitio web se comporta cuando es accedido, como por ejemplo con un modem.

- **Spider:** Identifica nuevas URLs en el sitio objetivo, y las recupera.

- **Solicitud Manual:** Permite editar y repetir un solicitud previa, o crear solicitudes completamente nuevas.

- **Análisis de IDs de Sesión:** Recolecta y analiza un número de cookies para determinar visualmente el grado de aleatoriedad y no predicibilidad.

Características (Cont.)

- **Scriptid:** Se puede usar BeanShell para escribir un script para crear solicitudes y traerlas desde el servidor. El script puede además realizar algún análisis sobre las respuestas, con todo el poder del modelo de objetos de solicitud y respuesta para simplificar las cosas.

- **Fuzzer de Parámetros:** Realizar substitución automática de valores de parámetros que son probables de exponer validación incompleta de parámetros, conduciendo a vulnerabilidades como XSS o SQLi.

- **Buscar:** Permite al usuario crear expresiones arbitrarias BeanShell para identificar conversaciones que deben ser mostradas en la lista.

- **Comparar:** Calcula la distancia de edición entre el cuerpo de la respuesta de la conversación observada, y la conversación seleccionada como referencia. La distancia de edición es “el número de ediciones requeridas para transformar un documento en otro”. Por razones de desempeño, las ediciones son calculadas utilizando tokens de palabras, en lugar de byte por byte.

Características (Cont.)

- **SOAP:** (Simple Object Access Protocol) Este plugin interpreta WSDL (Web Service Definition Language) y presenta varias funciones además de los parámetros requeridos, permitiendo editarlas antes de ser enviados al servidor. Se sugiere utilizar en su lugar SOAPUI.

- **Extensiones:** Automatiza las pruebas por archivos que son dejados por descuido en el directorio raíz del servidor web (.bak). Las verificaciones son realizadas para archivos y directorios. Las extensiones para archivos y directorios pueden ser editadas por el usuario.

- **XSS/CRFL:** Plugin de análisis pasivo que busca por datos controlados por el usuario en las cabeceras de respuesta HTTP y el cuerpo para identificar vulnerabilidades de inyección CRLF (Carriage Return and Line Feed) (HTTP response splitting) y XSS (Cross Site Scripting).

URL: http://www.soapui.org/

Curso Virtual de Hacking Aplicaciones Web

Días:

Grupo 1: Sábados 1, 8, 15 y 22 de Febrero del 2014
Grupo 2: Domingos 2, 9, 16 y 23 de Febrero del 2014

Horario:

De 9:00am a 12:30m (UTC -05:00)

Más Información:

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

caballero.alonso@gmail.com

@Alonso_ReYDeS

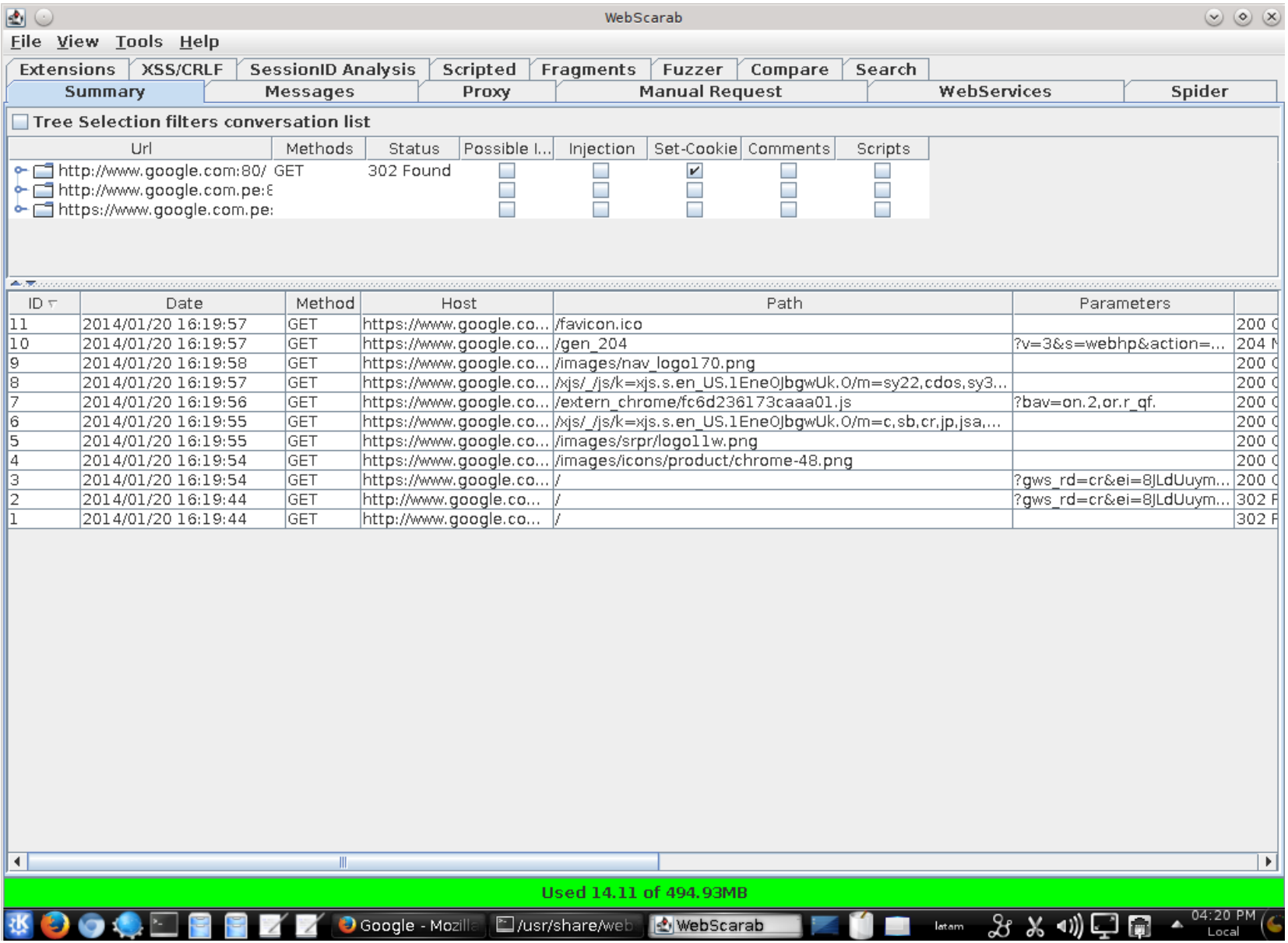
http://pe.linkedin.com/in/alonsocaballeroquezada/

ReYDeS

http://www.reydes.com

Demostraciones

A continuación se presentan algunas demostraciones prácticas utilizando OWASP WebScarab en Samurai-WTF



Más Material

Los invito a visualizar los 17 Webinars Gratuitos que he dictado hasta el momento, sobre temas de Hacking Ético, Pruebas de Penetración, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Pueden obtener todas las diapositivas utilizadas en los Webinars Gratuitos desde la siguiente página:

http://www.reydes.com/d/?q=node/3

Pueden obtener todos los artículos y documentos que he publicado.

http://www.reydes.com/d/?q=node/2

Mi blog personal:

http://www.reydes.com/d/?q=blog/1

¡Muchas Gracias!

OWASP WebScarab

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 30 de Enero del 2014